

**SECURE SYSTEM FOR THE CONTROL OF THE UNLOCKING OF AT
LEAST ONE OPENABLE PANEL OF A MOTOR VEHICLE**

5 The present invention relates to secure systems for the control of the unlocking of at least one openable panel of a motor vehicle.

10 In the remote control systems which are currently used for unlocking motor vehicle doors, the user must manually actuate his remote control (transmission/reception device integrated into the gripping part of his mechanical key) in order to actuate the unlocking of the doors.

15 Now, for greater user comfort, one wishes to eliminate manipulations of this type.

20 So-called "hands free" systems in which the user carries a transponder which is, for example, integrated into a badge have recently been proposed.

25 On receiving a radio frequency interrogation signal transmitted from the vehicle, the transponder transmits a radio frequency identification signal from itself in response. When this signal is received and identified by means provided for this purpose on the vehicle, these means order the unlocking of the openable panel.

30 Such a system is fully transparent to the user, since the unlocking of the doors is controlled without the user having to perform operations other than that consisting in his having to manipulate the handle of his door.

35 Such "hands free" systems pose security problems, however.

09883463 0622001
100290 0968860

5
10

15
20
25
30
35

30

35

in response which signal carries a pseudo-random code and which furthermore carries a signature which is specific to the said transmission/reception means of the user, the transmission/reception means on the
5 vehicle comprising means for de-spreading the signal received if the pseudo-random code carried by the said signal is synchronized with a corresponding pseudo-random code stored in their memory means and for verifying whether the signal received carries the
10 signature of the transmission/reception means of the user.

Other characteristics and advantages of the invention will further become apparent from the description which
15 follows which is purely illustrative and nonlimiting and which should be read in conjunction with the appended drawings, in which:

- Figure 1 is a schematic representation
20 illustrating a system in accordance with the invention;

- Figure 2 illustrates the function for correlating the pseudo-random codes cyclically permuted amongst themselves, used in a system of the type of that of
25 Figure 1.

Represented in Figure 1 is a vehicle V which carries RF transmission/reception means 1 intended to exchange with an RF transmission/reception module 2 carried by a
30 user and taking for example the form of a badge.

The transmission/reception means 1 comprise an antenna 3 disposed for example near a door handle of the vehicle, or in this handle, a management unit 5 as well
35 as signal conversion means 4 interposed between the antenna 3 and the management unit 5.

09883963-062001
T000290-19968880

The signal conversion means 4 comprise in particular means 6 for modulating or demodulating an RF signal transmitted or received by the antenna 3, a circular shift register 7 in which is stored a pseudo-random code, as well as mixer means 8 which are mounted between the management unit 5 and the said modulation/demodulation means 6 and which are able to mix the pseudo-random code with the signal demodulated by the means 6 or with a signal forwarded by the management unit 5. The pseudo-random code of the circular shift register 7 is cyclically permuted with itself at a certain clock frequency.

The badge 2 for its part comprises an antenna 9, a management unit 11 and signal conversion means 10 interposed between the antenna 9 and the management unit 11.

The signal conversion means 10 comprise, in the same way as the means 4, means 12 for modulating or demodulating an RF signal transmitted or received by the antenna 9, a circular shift register 13 in which is stored a pseudo-random code identical to that stored in the register 7, as well as mixer means 14 which are mounted between the management unit 11 and the said modulation/demodulation means 12 and which are able to mix the pseudo-random code with the signal demodulated by the means 12 or with a signal forwarded by the management unit 11. The pseudo-random code of the circular shift register 13 is cyclically permuted with itself at the same clock frequency as that of the shift register 7.

The vehicle V comprises means intended to make it possible to detect the presence of an individual near the vehicle. These means consist for example of sensors disposed in the handles of the doors and making it possible to detect the fact that an individual is

09883963-062001

1

5

This RF interrogation signal is a signal modulated by the means 6 which implement, for example, a 2-phase NRZ modulation. It carries the pseudo-random code stored in the register 7, mixed with a "challenge" code (key code) which is chosen by the management unit 5 from amongst several possibilities and which will have to determine the response which the badge 2 will have to give.

A hand-drawn diagram consisting of a central rectangular box labeled "badge". A line extends from the top-left corner of the box to a circle containing the number "9". Another line extends from the bottom-right corner of the box to a circle containing the number "2".

means 14 - the key code forwarded to the keypad?

substantially concomitantl
the antenna 3. Conversely,

accompany

[illegible]

More exactly, the correlation value varies, as a function of the phase shift between the pseudo-random code carried by the signal received and the pseudo-random code of the shift register 13, in the manner which is illustrated in Figure 2. It takes its maximum value when the two codes are perfectly synchronized and becomes a minimum for time shifts of at least one bit period. For time shifts of less than one bit period, it varies linearly between its maximum value and its minimum value.

Thus, there is substantially correlation between the two pseudo-random codes, for as long as the code received is shifted in time by less than half a bit period with respect to the code of the shift register 13 of the badge 2.

By way of example, the pseudo-random code can be coded on 127 bits, whilst the shift registers 7 and 13 are traversed at a clock frequency of 5 MHz, this corresponding to bit periods of 200 ns.

$$5 \times 10^6 \text{ Hz} = 200 \text{ ns/bit}$$

Correlations are then obtained at ± 30 m from the vehicle, (or subsequently at $7.62 \text{ km} \pm 30 \text{ m}$ or $15.24 \text{ km} \pm 30 \text{ m}$, etc.).

Once the key code has been recovered, the management unit 11 determines a secret code to be transmitted in the reverse direction. This secret code is a code which the said vehicle V expects to receive and which is dependent on the key code forwarded by the vehicle V.

This secret code is subsequently mixed with the pseudo-random code of the shift register 13, then the signal obtained is modulated by the means 10 and transmitted by the antenna 9.

09883963-062001

$5 \times 10^6 \times 200 \times 10^{-9}$
= 1 bit

In particular, when a key code is used at the level of the vehicle, the latter might not be mixed with the pseudo-random code but consist of a pseudo-random code chosen from among several which are possible. Likewise, the secret code transmitted by the badge 2 might not be a code mixed with a pseudo-random code, but consist of a pseudo-random code specific to the badge 2, which consequently intrinsically carries the latter's signature. The means 1 then comprise means, synchronized with the badge 2, which are able to de-spread the signal received with this pseudo-random code.

Moreover, a possible sequence for the synchronization between shift registers of the means 1 and of the badge 2 may be as follows.

When the presence of an individual near the vehicle is detected, the vehicle transmits an activation signal intended to wake up the badge 2.

On receipt of this activation signal, the badge 2 transmits an RF signal which carries an identification code mixed with a short pseudo-random signal ("short" to be understood in contradistinction to the 'long pseudo-random signal, in this instance 127 bits long, used after the synchronization step).

The identification code is used to avoid the situation in which vehicles other than the one concerned respond upon the activation of the badge 2. It is repeated over a period sufficient for the transmission/reception means 1 of the vehicle V to self-synchronize with the pseudo-random signal.

35

When such is the case, the transmission/reception means 1 transmit a response signal which marks the end of the initialization sequence. So long as this response of

T00290-EG6E860

the vehicle is not received by the badge 2, the latter repeats the transmission of the signal which carries the identification code mixed with a short pseudo-random signal.

5

T00290" E96E9860